楕円曲線の導手の体拡大による変化について (ディオファントス問題と解析的整数論)

AUTHOR(S):

木田, 雅成

CITATION:

木田, 雅成. 楕円曲線の導手の体拡大による変化について (ディオファントス問題と解析的整数論). 数理解析研究所講究録 2003, 1319: 56-60

ISSUE DATE:

2003-05

URL:

http://hdl.handle.net/2433/43050

数理解析研究所講究録 1319 巻 2003 年 56-60

楕円曲線の導手の体拡大による変化について

木田雅成 (Masanari Kida)
電気通信大学
(University of Elecctro-Communications)

1 定義と問題

$\mathbb{Q}_p$ を p 進体とし, K をその有限次拡大体とする. 本稿では $\mathbb{Q}_p$ の分離閉包 $\overline{\mathbb{Q}_p}$ を一つ固定し, すべての $\mathbb{Q}_p$ の代数拡大は $\overline{\mathbb{Q}_p}$ に含まれていると仮定する.

E を K 上定義された楕円曲線とし, ℓ を p と異なる素数とする. E の等分点を添加して得られる体 $D = K(E[\ell])$ を E の ℓ 等分点の体という. D/K は正規拡大で, その Galois 群 $G = \mathrm{Gal}(D/K)$ は $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ の部分群に同型であることが知られている. G_i を G の高次分岐群とするとき, E の導手の wild part が

$$\delta(E/K) = \sum_{i=1}^{\infty} \frac{\#G_i}{\#G_0} \dim_{\mathbb{Z}/\ell\mathbb{Z}} \left(E[\ell]/E[\ell]^{G_i} \right)$$

と定義される. この定義において, 高次分岐群が十分大きなところでは自明になることから, 和は実際には有限和である. さらにこの量が ℓ によらずに決まる非負整数であることが知られている. Néron-Ogg-Shafarevich の判定法により E が good reduction を持てば, D/K が不分岐であることがわかるので, このとき $\delta(E/K) = 0$ である. また $\delta(E/K)$ の定義から, D/K が tamely ramified なら $\delta(E/K) = 0$ であることが直接導かれる. したがって $\delta(E/K)$ は E が bad reduction をもつときに, その程度を分岐によって示す量である.

さて, ここで問題にするのは M/K を有限次拡大とするとき base change

$$E_M = E \times_{\mathrm{Spec}(K)} \mathrm{Spec}(M)$$

の導手の wild part $\delta(E_M/M)$ を記述することである.

E の導手の tame part $\varepsilon(E/K)$ は

$$\varepsilon(E/K) = \begin{cases} 0 & E \text{ が good reduction のとき} \\ 1 & E \text{ が multiplicative reduction のとき} \\ 2 & E \text{ が additive reduction のとき} \end{cases}$$

と定義されるが, この量が base change でどのように変化するかは stable reduction theorem によってある程度わかる. したがってここで考える問題は stable reduction theorem の wild part 版とみることができる.

K の剰余標数 p が 5 以上の時は Ogg, Serre-Tate によって wild part は常に 0 であることが知られている. したがって, 問題になるのは $p = 2, 3$ の場合である. 以下の章では, 専らこれらの場合を考える.

本節で引用したの楕円曲線に関する事実については [5], [6] を参照されたい.

2 $\delta(E/K)$ の公式

L/K が局所体の有限次 Galois 拡大の時に, Galois 群 $G = \mathrm{Gal}(L/K)$ の部分群として高次分岐群 G_i が定義される. さらに, 良く知られているように Hasse-Herbrand の関数を $\psi_{L/K}$ とするとき $G^x = G_{\psi_{L/K}(x)}$ によって上つき番号の高次分岐群が定義される. このとき

$$\mathcal{U}(L/K) = \{t \in [-1, \infty) \mid G^t \neq G^{t+\varepsilon} \text{ for } \forall \varepsilon > 0\},$$

さらに

$$\mathrm{u}(L/k) = \max \mathcal{U}(L/k)$$

で $\mathcal{U}(L/K)$ と $\mathrm{u}(L/k)$ を定義する. この記号の下で次の補題が成立する.

補題 1. $p = 2, \ell = 3$ として $K \supset \mathbb{Q}_2, D = K(E[3])$ とすると

$$\delta(E/K) = 2 \times \mathrm{u}(D/K)$$

が成立する. $p = 3, \ell = 2$ としても同じ式が成り立つ.

この補題によれば有限次拡大 M/K に対して $\delta(E_M/M)$ を計算するには $\mathrm{u}(DM/M)$ が計算できれば良いことになる.

3 やさしい場合

一般に二つの代数体が与えられているときに, その合併体の分岐を調べることは難しい問題であって, 一般的な方法は知られていないが, 以下の二つの場合には, 簡単に計算できる.

3.1 Tamely ramified の場合

M/K が tamely ramified なら Herbrand の定理を使った議論により, $e(M/K)$ を分岐指数とすると,

$$\mathrm{u}(DM/M) = e(M/K)\mathrm{u}(D/K)$$

が成り立つので, 補題 1 より, きれいな関係式

$$\delta(E_M/M) = e(M/K)\delta(E/K)$$

が得られる.

3.2 Arithmetically disjoint の場合

補題 2 (Maus [3]). K_1/k, K_2/k を局所体の有限次完全分岐拡大で *linearly disjoint* なものとする. $\mathcal{U}(K_1/k) \cap \mathcal{U}(K_2/k) = \emptyset$ ならば

$$\mathcal{U}(K_1K_2/K_1) = \{\psi_{K_1/k}(u) \mid u \in \mathcal{U}(K_2/k)\}.$$

$\mathcal{U}(K_1K_2/K_2)$ も同様の記述ができる.

この補題の条件が満たされる時, K_1 と K_2 は k 上 arithmetically disjoint という.

$\mathcal{U}(D/K)$ と $\mathcal{U}(M/K)$ がわかっていれば, どの場合に arithmetically disjoint になるのかは直ちに判定できて, その場合には $\delta(E_M/M)$ が計算できる.

4 主結果

以上に述べたことから, D/K, M/K がともに wild ramification を含む場合が問題として残るわけであるが, この場合に一般的で単純な記述を与えることはいまだできていない. 本稿での主結果は $K = \mathbb{Q}_p$ で $M/\mathbb{Q}_p$ が p 次の完全分岐拡大の場合の完全な記述である.

$p = 2$ の場合にのみに定理を述べる. $p = 3$ の場合には, より簡単な同様の定理が成立する.

定理 3. $E/\mathbb{Q}_2$ を *additive reduction* をもつ楕円曲線とする. E の 3 等分点の体 D が $\mathbb{Q}_2$ 上 *wildly ramified* であると仮定する. $\mathbb{Q}_2$ 上の分岐二次拡大を次の三つにわける.

$$\Omega_1 = \{\mathbb{Q}_2(\sqrt{-1}), \mathbb{Q}_2(\sqrt{3})\},\ \Omega_2 = \{\mathbb{Q}_2(\sqrt{2}), \mathbb{Q}_2(\sqrt{10})\},\ \Omega_3 = \{\mathbb{Q}_2(\sqrt{-2}), \mathbb{Q}_2(\sqrt{6})\}.$$

$M \in \Omega_i$ のとき $\delta(E_M/M)$ は次の表で与えられる.

$\delta(E/\mathbb{Q}_2)$	$\mathrm{Gal}(D/\mathbb{Q}_2)$	Ω_1	Ω_2	Ω_3
1		1	1	1
2	$\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$	1	2	2
	その他	0	2	2
3		4	3	3
4	$\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$	6	$\begin{cases} 2 \\ 1 \end{cases}$	$\begin{matrix} 1 \\ 2 \end{matrix}$
	SD_{16}	6	3	3
	その他	6	$\begin{cases} 2 \\ 0 \end{cases}$	$\begin{matrix} 0 \\ 2 \end{matrix}$
5		8	6	6
6		10	8	8

ここで $\delta(E_M/M)$ に二つの可能性がある場合にも, D に関する情報がもうすこし余分にあればどちらが起こるかを決めることができる.

定理の証明では, まずどの場合が arithmetically disjoint になるかを決めるために $\mathcal{U}(D/\mathbb{Q}_2)$ を計算する.

命題 4. E を $\mathbb{Q}_2$ 上で定義された *additive reduction* をもつ楕円曲線とする. 3 等分点の体 $D/\mathbb{Q}_2$ が *wildly ramified* とする. L を第一高次分岐群 $G_1(D/\mathbb{Q}_2)$ の固定体とする. このとき導手と *Galois* 群の間には次の対応関係がある.

$\delta(E/\mathbb{Q}_2)$	$\mathrm{Gal}(D/\mathbb{Q}_2)$	$\mathrm{Gal}(D/L)$	$\mathcal{U}(D/L)$
1	$\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$	Q_8	$\left\{1, \frac{3}{2}\right\}$
2	$\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$	Q_8	$\{1,3\}$
	D_{12}	C_2	$\{3\}$
	C_8	C_2	$\{1\}$
	E_4	C_2	$\{1\}$
3	SD_{16}	Q_8	$\left\{1, \frac{3}{2}\right\}$
4	$\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$	Q_8	$\{1,6\}$
	D_{12}	C_2	$\{6\}$
	SD_{16}	Q_8	$\{1,2\}$
	C_8	C_2	$\{2\}$
	E_4	C_2	$\{2\}$
5	$\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$	Q_8	$\left\{5, \frac{15}{2}\right\}$
6	SD_{16}	Q_8	$\{1,2,3\}$
	C_8	C_4	$\{2,3\}$
	D_8	C_4	$\{2,3\}$

この命題は [4] や [1] で得られている結果と関連がある. この命題によれば導手と Galois 群 $\mathrm{Gal}(D/\mathbb{Q}_2)$ の同型類 (それは 3 等分方程式から容易に計算できる) が与えられれば, その分岐は完全に決まってしまう. したがって, 例えば与えられた判別式をもつ $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ 拡大を与える楕円曲線が導手よって完全に特徴づけられることになる.

この命題の証明は Galois 群の同型類一つ一つについて群論的な制限から高次分岐群を決めていくことでなされる.

残りの arithmetically disjoint でない一般の場合には基礎体が $\mathbb{Q}_2$ であることを利用し, その上の小さな次数の拡大体の個数などを利用して, うまく分岐を計算する. ここでは拡大 $D/\mathbb{Q}_2$ が楕円曲線の等分点からできていることを利用して証明できる場合を簡単に紹介する.

$\mathrm{Gal}(D/\mathbb{Q}_2) \cong \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ の場合を考える. この場合 D の部分体で $\mathbb{Q}_2$ 上 Galois

になるものは

$$\mathbb{Q}_2 \subset \mathbb{Q}_2(\sqrt{-3}) \subset F \subset D_x \subset D$$

となる. ここで $D_x = \mathbb{Q}_2(x(E[3]))$ である. D と MD_x が D_x 上で arithmetically disjoint にならずに Maus の定理 (補題 2) が適用できない場合には次のようにする.

Weil [7] によって D が具体的な楕円曲線 W の 3 等分点の体として実現可能であることがわかっている. また簡単な考察から DM/D_x の中間体として W の $M/\mathbb{Q}_2$ に関する twist W^M の 3 等分点の体が含まれている. よって Tate のアルゴリズムをつかって W^M の導手を計算すると, 逆に $\mathfrak{u}(\mathbb{Q}_2(W^M[3])/D_x)$ が計算できて, うまくいけば $\mathbb{Q}_2(W^M[3])$ と MD_x が D_x 上 arithmetically disjoint になることによって $\mathfrak{u}(DM/MD_x)$ が計算できる. これから $\mathfrak{u}(DM/M)$ を復元することはそれほど難しくない.

詳しい計算については [2] を参照のこと.

以上で述べた結果は, 非自明な場合のうち, もっとも単純な場合であるが, それでも結果は複雑である. K を $\mathbb{Q}_p$ より大きくしたりすると, その上の拡大が多くなることから, wild part の変化の記述は, よりいっそう複雑になると考えられ, その場合には記述に必要なデータも多くなると思われる. それを考慮すると, 一般の場合に「単純な」記述はあまり期待できないように思われる.

最後に少し応用を述べる. $\delta(E_M/M)$ が記述できると Ogg の公式

$$\varepsilon(E_M/M) + \delta(E_M/M) = v(\Delta_M) + 1 - m$$

によって多くの場合に m が計算できる. ここで Δ_M は E_M の極小判別式で, m は minimal proper regular model の special fibre の irreducible component の数である. m がわかると, ほぼ E_M の reduction type が決まってしまう. これから上で述べた結果を使って, 楕円曲線の reduction の base change に関する変動を記述することが多くの場合に可能になる.

参考文献

[1] P. Bayer and A. Rio, *Dyadic exercises for octahedral extensions*, J. Reine Angew. Math. **517** (1999), 1–17.

[2] M. Kida, *Variation of the reduction type of elliptic curves under small base change with wild ramification*, Preprint (2003).

[3] E. Maus, *Arithmetisch disjunkte Körper*, J. Reine Angew. Math. **226** (1967), 184–203.

[4] H. Naito, *Local fields generated by 3-division points of elliptic curves*, Proc. Japan Acad. Ser. A Math. Sci. **78** (2002), 173–178.

[5] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1986.

[6] ———, *Advanced topics in the arithmetic of elliptic curves*, Springer-Verlag, New York, 1994.

[7] A. Weil, *Exercices dyadiques*, Invent. Math. **27** (1974), 1–22.

(講演 2002 年 10 月 22 日)

e-mail: kida@sugaku.e-one.uec.ac.jp